

DPMSG



Digital Property Market Steering Group

Smart Property Data Trust Framework Sandbox



Regulating
Property
And
Probate
Lawyers



Open Property
Data Association

RAIDIAM

Introduction to the Sandbox Setup Guide

Contents

Introduction	3
How to Obtain Help & Support:	3
Sandbox Overview	4
How to sign up to the Sandbox	5
High Level Steps	5
Roles Within the Sandbox	5
The Pre-requisites	6
Getting Started: Data Provider	6
Getting Started: Data Receiver	8
Setting up your Sandbox Account	8

Introduction

The Smart Property Data Trust Framework Prototype (which we refer to as ‘the sandbox’) is a shared trust layer that enables organisations involved in the property ecosystem to securely discover, trust, and exchange data with one another to simplify and support the homebuying process.

The sandbox technically enforces and assures the rules of participation for the property ecosystem as determined by the scheme operator – for the sandbox this is OPDA.

The sandbox means that organisations don’t need to create multiple bilateral contracts and integrations with each other, to engage in complex, multi-party property journeys. Instead, the contract is managed at the scheme level, and the sandbox enables members to trust other members of the scheme, and connect to each other directly, using a standardised, secure integration format.

The [Smart Property Data Trust Framework](#) booklet from the DPMSG has more background on the trust framework approach, and the sandbox. More information is also available at the project’s [website](#), courtesy of The Council For Licenced Conveyancers (CLC).

How to Obtain Help & Support:

This is a pilot and we support members of all levels of technical capability to participate, and we recognise you and/or your organisation may not feel technically ready. The sandbox is designed to uncover any issues in a safe, non-production environment, and highlight ways to improve the process.

We are here to help. If you are having problems with any step during this guide, please email the appropriate contact:

RAIDIAM Technical lead: alan.hughes@raidiam.com

RAIDIAM Programme Manager: anthony.jones@raidiam.com

OPDA Contact: paul@openpropdata.org.uk

Sandbox Overview

The property buying and selling process involves many different organisations - estate agents, conveyancers, lenders, search providers, and more - each holding pieces of information that others need. Today, sharing that information is often slow, manual, and difficult to verify. The sandbox exists to change that.

The sandbox is a secure, governed ecosystem that allows organisations involved in property transactions to share data with each other safely and efficiently. Crucially, it also makes it possible to verify where data came from and whether it can be trusted - something that is increasingly important as property transactions become more complex and more digital.

What the Sandbox enables

The sandbox gives OPDA, as the scheme owner, a way to put the agreed rules of the ecosystem into practice and ensure all members are following them. In practical terms, this means that organisations are properly checked and approved before any data is shared and that members can find each other through a shared directory and exchange data directly, according to the permissions they hold. Different roles allow different organisations to access the right information for their needs, and an organisation can hold more than one role. Where trusted information already exists, it is reused rather than recreated - reducing errors and saving effort. And every action is recorded, so there is always a clear picture of who did what and when.

Core Benefits

The sandbox delivers a number of important capabilities that underpin the whole ecosystem:

- **Directory of Trusted Members** - a single, reliable list of all approved organisations and what they are permitted to do.
- **Identity, Trust, and Accreditation** - every organisation is verified, approved, and held to the same agreed standards before participating.
- **Secure Access and Authorisation** - access to data is protected consistently across the entire network, so there are no weak links.
- **A Common Foundation of Trust** - because all members trust the same shared framework, organisations can trust each other without needing to establish separate agreements with every other participant they interact with.
- **Data Provenance** - it is always clear who created a piece of information, when they created it, and how trustworthy it is. This is central to the OPDA mission.
- **Non-Repudiation and Auditability** - when data is received, the framework provides tools such as digital signatures that allow the recipient to verify it came from a trusted and approved source, and that it has not been tampered with along the way.

How to sign up to the Sandbox

High Level Steps

1. Discuss your participation with Paul Albone at OPDA (paul@openpropdata.org.uk).
 - Paul will help you determine [the role\(s\)](#) (e.g., *Data Provider*, *Data Receiver*, or both) that your organisation will need to participate on the sandbox.
2. Review the [pre-requisites](#) for the role your organisation will adopt, alongside your technical team, and engage Raidiam contacts as required if any help is needed.
3. Confirm your wish to participate by emailing Paul Albone at OPDA, notifying him of the primary contact/administrator for your organisation.
 - This person will be set up for your firm, and then be able to create other users and complete onboarding for your organisation.
 - Paul will also provide Ts&Cs for your participation on the sandbox.
 - Complete the [onboarding questionnaire](#), which helps Raidiam understand your organisation's technical situation and readiness for sandbox participation.
4. Your nominated administrator will receive an email with instructions on how set up their own multi factor security access for the sandbox.
5. Confirm that the pre-requisite requirements for your role are implemented (reach out to Raidiam should you require any assistance).
6. Your administrator will need to log on to the sandbox to continue to set-up your organisation, by registering your organisations API's in the sandbox (we can help with this if needed).

Note: This guide covers steps 1-4 above. Steps 5 and 6 are explained in the [Introduction to the Sandbox: Technical Guide](#).

Roles Within the Sandbox

The trust framework defines clear, reusable roles to ensure members can only interact and securely share data with other members that they have permission to engage with. OPDA will work with you to clarify which of the following role profiles suits your organisation's needs:

- **Data Provider:** Organisations that share data in the framework, including data they get from official sources or create from that official data e.g. GroundSure, Mining Remediation Authority, Ordnance Survey, Mortgage Lenders, etc. Some of these data providers will be

Source Data Providers, organisations that create and hold the original, official property information e.g. HMLR.

- **Data Receiver:** Organisations that use the data in the framework to provide services or make decisions. For example, Digital Property Pack Providers, Estate Agents, Conveyancers, etc.

Organisations **may hold multiple roles**, enabling them to act differently according to their need within a particular stage in the process, for example consuming data in one context and providing data for other members to use in another context.

The final role is for the Scheme Operator. The **Trust Framework Administrator** sets the rules for how the sandbox works, makes sure they are followed, and approves which organisations can take part. For the sandbox this is OPDA and Raidiam together.

The Pre-requisites

Getting Started: Data Provider

To join the sandbox as a *Data Provider*, there are a few steps to get set up securely. These steps exist to keep data safe and make sure only verified members can connect.

How the sandbox works

The sandbox lets members share data with each other through secure digital connections using Application Programming Interfaces (APIs). It keeps a directory of all members and their connection details, sets minimum security standards everyone must follow, and allows members to connect directly with each other to share data. One important thing to know: **your data never passes through the sandbox itself** - it goes directly between you and the other member.

What you'll need to get set up

There are two things required to get connected:

1. **An Authorisation Server** - this manages who is allowed to access your data. You can either set up your own or use one provided by Raidiam.
2. **A secure mutual Transport Layer Security (mTLS) gateway** - this acts as a digital doorman, checking certificates to verify that whoever is connecting is who they say they are.

Don't worry if this sounds unfamiliar - you can choose the setup path that works best for you, and we'll be with you every step of the way with guidance, examples, and hands-on support.

1. Authorisation Server for Secure Access Management

Your Application Programming Interfaces (APIs) must be protected by an Authorisation Server that manages *who* can connect and *how*.

Your options:

1. **Use your own Authorisation Server** (must be OAuth2.0 and support automated onboarding known as *Dynamic Client Registration*).
2. **Use the Raidiam Connect Authorisation Server**, where registration and security setup are already handled.

How we'll help: We will provide guidance and examples for setting up your own secure authorisation system. We can also provide full onboarding support if you choose the Raidiam Connect option.

2. mTLS Gateway for a Secure Connection Channel

All data traffic must pass through a secure gateway that checks digital certificates - a process known as mutual TLS (mTLS). This ensures that only verified participants can connect to your APIs.

For your gateway, we strongly recommend using **nginx** (or a similar reverse proxy). This is a reliable option and the one we're best placed to support.

If you're already using Amazon Web Services (AWS) that's fine - AWS works well for many parts of your setup. However, **we'd advise against using the AWS Application Load Balancer (ALB) as your mTLS gateway specifically**, as it has limitations around real-time certificate checks that can cause compliance issues. You're welcome to use AWS infrastructure in other areas of your system.

How we'll help: We'll provide sample configurations and step-by-step guidance to get your mTLS gateway set up, along with support to validate certificates and make sure everything meets the sandbox standards.

3. Suggested Setup

One approach that works well is pairing two components that each handle a distinct job:

- **nginx** as your mTLS gateway - acting as the secure entry point that checks digital certificates before any connection is established.
- **AWS API Gateway with a Lambda Authoriser** - handling the deeper security checks once a connection is allowed through.

This combination offers real-time verification of participant certificates, full control over your validation logic, better logging, and confidence that your setup will stay compliant as security standards evolve.

How we'll help: We'll provide sample Go code and nginx configurations to illustrate this approach. If you're using a different environment or cloud provider, we're happy to help you find an equivalent setup that works for you.

Getting Started: Data Receiver

To get started as a *Data Receiver*, you simply need to be invited to join the sandbox. Unlike the *Data Provider* role, there are no additional technical setup requirements to meet before you can get started.

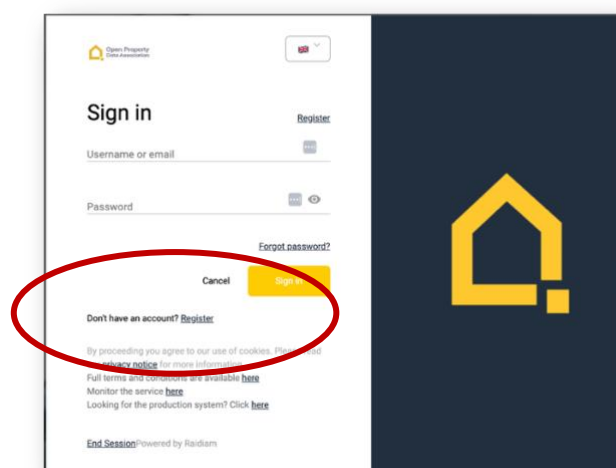
The [Introduction to the Sandbox: Technical Guide](#) provides instructions to enable you to set up your organisation so that it can start receiving data from *Data Providers*.

Setting up your Sandbox Account

Once the OPDA team has granted you access, you'll receive an email from directoryservices@raidiam.com with the subject line "**Raidiam Sandbox - Your access to Raidiam**". Click the "Go to the platform" link in that email to reach the sandbox registration page.

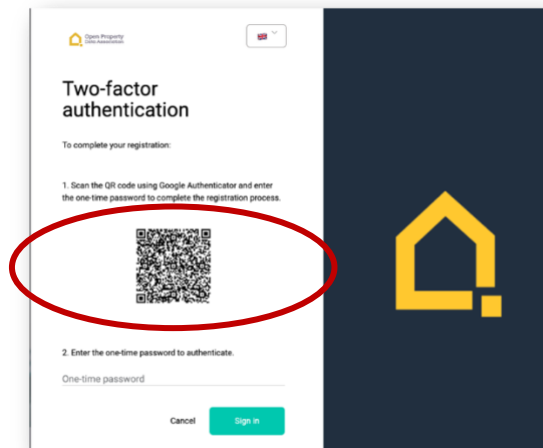
Note: If you can't find the email, it's worth checking your spam or junk folder.

1. Click on "Register" to create a new user account.

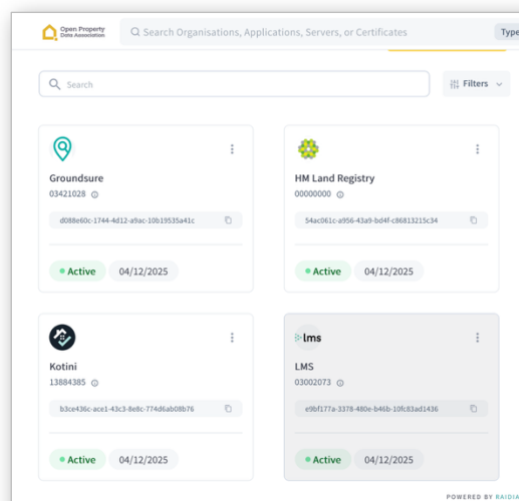


2. Fill in your personal details and click **Register**. A one-time password (OTP) will be sent to your email address — enter this to complete your registration. If the OTP doesn't arrive, click "**Resend OTP**" and check your spam folder if needed.

- Using an authenticator app on your phone (such as Google Authenticator), scan the QR code shown on screen and enter the one-time password it generates. You only need to set this up once. After this, each time you sign in, or when your session has expired, you will be prompted to enter a code or password generated from your authenticator app.



- Once you've registered, set up MFA, and been invited to an organisation, you'll be taken to the directory. If you run into any problems or can't get access, just get in touch with the OPDA project team.



Note: Once your first organisation administrator has been set up, they can invite additional administrators to the organisation by following these steps: [Add Organisation Admins](#).

That's it for the administrator setup!

Once you've completed the steps above, you're ready to log in to the sandbox and move on to the next stage: generating your certificates, registering servers, and registering your applications. Step-by-step instructions for each of these tasks can be found in the [Introduction to the Sandbox: Technical Guide](#), which also contains a glossary if needed.